Ville Impiö

Tietoturvakartoitus yritykselle

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

11.5.2015

Metropolia

Tekijä Otsikko Sivumäärä Aika	Ville Impiö Tietoturvakartoitus yritykselle 33 sivua 11.5.2015
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja	lehtori Kimmo Saurén

Tämän insinöörityön aiheena oli tietoturvakartoituksen tekeminen yritykselle. Työssä käsiteltiin ja tutkittiin yrityksen tietoturvaa pohjautuen tietoturvan eri osa-alueisiin ja määritelmään. Teoriaosuudessa käsiteltiin tietoturvaa yleisellä tasolla, tietoverkkojen toimintaa ja rakennetta, sekä penetraatiotestausta osana tietoturvakartoitusta. Tietoturvakartoitus tehtiin toimeksiantona kansainväliselle monialayritykselle ja se oli osa Metropolian laajempaa yhteistyöprojektia, johon kuuluu useita yrityksiä.

Työn tavoitteena oli selvittää yrityksen tietoturvan nykyinen tila ja puutteet sekä pohtia kehityskohtia tietoturvan parantamiseksi yrityksessä. Tietoturvakartoitus perustui tässä tapauksessa yrityksen luovuttamiin tietoihin sekä omiin yritysvierailuiden aikana tehtyihin testauksiin ja havaintoihin. Tunkeutumistestaus tehtiin osittain yrityksen etukäteen luovuttamien tietojen perusteella ja osittain testaajan itse selvittämien tietojen perusteella.

Yrityksen tietoturvan yleisen tason kartoituksessa havaittiin, että tietoturva on pääosin hyvällä tasolla ja käytännön asiat on mietitty tarkoin. Suurimmaksi puutteeksi nähtiin se, ettei henkilöstölle järjestetä minkäänlaista tietoturvakoulutusta. Käytännön testausosuudessa tehtiin yrityksen sisäverkkoon ja työasemaan kohdistuvia testauksia. Testauksissa saatiin selville että tietoturva on näiltä osin mietitty suhteellisen pitkälle, mutta joitain heikkouksiakin löydettiin esimerkiksi sisäverkon rakenteesta ja käyttöjärjestelmistä.

Tuloksena syntyi siis tavoitteen mukaisesti tietoturvallisuuden puutteita. Tulosten perusteella pystyttiin pohtimaan kehitysehdotuksia yrityksen tietoturvalle ja yhteenvetona voidaan todeta insinöörityön tavoitteiden täyttyneen.

Avainsanat	tietoturva, tietoverkot, penetraatiotestaus

Author	Ville Impiö
Title	Information security survey for a company
Number of Pages	33 pages
Date	11 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Networks
Instructor	Kimmo Saurén, Senior Lecturer

The goal of this final year project was to carry out an information security survey for a company. The information security of the company was examined based on different aspects and definitions of information security. The theoretical part of the thesis contains a description of the general level of information security, network operations and penetration testing as part of the information security analysis. The practical work was done under a contract for an international company, and it was part of a larger cooperation project of Metropolia that includes a number of companies.

This information security survey consists of an examination of the company's overall level of information security and penetration testing on the company's internal network. In this case, general information security survey and penetration testing was done partly based on information the company had provided beforehand and mainly based on information that was gathered by tester himself.

The objective of this thesis was to examine the current level of the information security of the company and to consider which issues would require improvements. As a result, several security threats were found and suggestions for improvement were made.

Keywords	information security, network, penetration testing

Sisällys

Lyhenteet

ARP	Tietoliikenneprotokolla, jolla selvitetään IP-osoitetta vastaava MAC-osoite
BIOS	Basic Input-Output System. Tietokoneohjelma, joka lataa käyttöjärjestelmän keskusmuistiin ja käynnistää sen.
Brute force	Väsytysmenetelmä, jossa tietokone kokeilee kaikki mahdolliset merkkiyhdistelmät löytääkseen salasanan.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteeksi.
DOS	Denial of Service. Palvelunestohyökkäys jossa estetään palvelun tai verkkosivuston käyttö.
FTP	File Transfer Protocol. TCP-protokollaa käyttävä tiedonsiirtomenetelmä kahden laitteen välillä.
HTTP	Hypertext Transfer Protocol. Tietoliikenneprotokolla jota selaimet ja palvelimet käyttävät tiedonsiirtoon.
ICMP	Internet Control Message Protocol. Yksinkertainen protokolla IP-verkkojen saavutettavuuden raportointia varten.
IDS	Intrusion Detection System. Tunkeilijan havaitsemisjärjestelmä on tietoverkon järjestelmä, joka tunnistaa hyökkäysyrityksiä.
IP	Internet Protocol. Tietoliikenneprotokolla, joka huolehtii IP-pakettien perille toimittamisesta. IP-paketti on Internet-protokollan perusyksikkö.
IPS	Intrusion Prevention System. Aktiivinen murron estämisjärjestelmä, joka katkaisee hyökkääjän yhteydet.
LAN	Local Area Network. Lähiverkko on määrätyllä alueella toimiva tietoliikenneverkko.

MAC	Media Access Control. Verkkosovittimen yksilöivä fyysinen osoite.
OSI	Open Systems Interconnection. Malli, joka kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
PSK	Pre-Shared Key. WLAN-verkoissa käytettävä salasana.
SMTP	Simple Mail Transfer Protocol. TCP-protokolla, jota käytetään sähköpostipalvelimien viestien välitykseen.
SNMP	Simple Network Management Protocol. Verkkojen hallinnassa käytettävä tietoliikenneprotokolla.
STP	Spanning Tree-protokolla on kytkimien käyttämä toiminto, jonka avulla estetään verkon silmukoita.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jolla luodaan yhteyksiä laitteiden välille.
UDP	User Datagram Protocol. Yhteydetön tietoliikenneprotokolla, joka mahdollistaa tiedon siirron ilman laitteiden välistä yhteyttä.
VLAN	Virtual LAN. Virtuaalilähiverkko on tekniikka, jolla fyysinen verkko voidaan jakaa pienempiin osiin.
VPN	Virtual Private Network. Virtuaalinen erillisverkko on tapa, jolla yksityisiä verkkoja voidaan yhdistää julkisen verkon yli.
WLAN	Wireless LAN. Langaton lähiverkko, jossa laitteet voidaan yhdistää ilman kaapeleita.

1 Johdanto

Tietoturva on erittäin tärkeä osa-alue nykyajan yritystoimintaa organisaation kokoluokasta riippumatta. Tärkeät ja salaisiksi tarkoitetut tiedot täytyy suojata niin, että ne eivät päädy ulkopuolisten tai kilpailevien yrityksien käsiin. Yrityksen tietoturva mielletään usein vain tietokoneisiin ja tekniikkaan liittyväksi asiaksi, jonka tehtävänä on torjua viruksia käyttäjän työasemalla. Nykykäsityksen mukaan tietoturvan nähdäänkin kattavan kaiken, kulunvalvonnan ja sähköpostin välillä.

Tämä insinöörityö tehdään toimeksiantona kansainväliselle monialayritykselle, ja se on osa Metropolian laajempaa yhteistyöprojektia, johon kuuluu useita yrityksiä. Työssä käsitellään ja tutkitaan yrityksen tietoturvaa pohjautuen tietoturvan eri osa-alueisiin. Työn teoriaosuudessa käsitellään tietoturvaa yleisellä tasolla, tietoverkkojen toimintaa ja rakennetta sekä penetraatiotestausta osana tietoturvakartoitusta.

Tietoturvakartoitus koostuu yrityksen yleisen tietoturvatason tutkimisesta, yrityksen sisäiseen tietoverkkoon kohdistuvasta tunkeutumistestauksesta sekä yrityksen työasemien tietoturvatason kartoittamisesta. Yleinen tietoturvan kartoitus perustuu tässä tapauksessa yrityksen luovuttamiin tietoihin sekä omiin yritysvierailuiden aikana tehtyihin havaintoihin. Tunkeutumistestaus tehdään osittain yrityksen etukäteen luovuttamien tietojen perusteella ja osittain testaajan itse selvittämien tietojen perusteella. Yrityksen kannettavan tietoturvatestauksessa simuloidaan tilannetta, jossa yrityksen kannettava on varastettu. Työn tavoitteena on selvittää yrityksen tietoturvan nykyinen tila ja pohtia kehityskohtia tietoturvan parantamiseksi.

2 Tietoturvallisuus

2.1 Tietoturvallisuuden määritelmä

Tietoturvallisuuden perinteisessä määritelmässä tietoturva koostuu kolmesta osatekijästä: luottamuksellisuudesta (confidelity), käytettävyydestä (availability) ja eheydestä (integrity).

Luottamuksellisuudella tarkoitetaan sitä, että tietojärjestelmän tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä. Käytettävyys on sitä, että tiedot ovat saatavissa tietojärjestelmästä riittävän nopeasti ja oikeassa muodossa. Eheydellä viitataan siihen, että tietojärjestelmän sisältämät tiedot pitävät paikkansa eivätkä ne sisällä virheitä. (1.)

Luottamuksellisuutta ylläpidetään suojaamalla tietojärjestelmien laitteet ja tietovarastot käyttäjätunnuksilla ja salasanoilla. Käytettävyyden takaamiseksi pidetään huoli siitä, että järjestelmien laitteet ovat riittävän tehokkaita ja ohjelmistot ovat sopivia järjestelmän tietojen käsittelyyn.

Eheyteen pyritään pääasiassa ohjelmistopuolen ratkaisuilla, esimerkiksi sovelluksiin sisällytetään erilaisia syöttörajoitteita tai syötteen tarkistuksia, kun taas tallennus- ja tiedonsiirto-operaatioihin varmistussummia tai tiivisteitä. Laitteistotasolla pyritään estämään virheet käyttämällä esimerkiksi virheen korjaavia muisteja tai väyliä. Tietoliikenneratkaisuissa suositaan virheen tunnistus- ja korjausmekanismeilla varustettuja protokollia ja laitteita. Useimmat salakirjoitusmenetelmät ja -tuotteet soveltuvat myös eheyden ylläpitoon. (1.)

2.2 Tietoturvan osa-alueet

Tietoturvan osa-alueet voidaan jakaa pienemmiksi kokonaisuuksiksi. Lähteestä riippuen osa-alueita on yleensä joko seitsemän tai kahdeksan. Osa-alueet ovat usein kytköksissä toisiinsa ja ne vaikuttavat toisiinsa eri tavoin tilanteesta riippuen. Tässä työssä käytetään mallia, jossa tietoturva on jaettu seitsemään osa-alueeseen:

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöturvallisuus

- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus.

Hallinnollinen turvallisuus

Hallinnollinen turvallisuus on tietoturvan kehittämisen ja johtamisen varmistamista. Siihen liittyvät myös yhteydenpito eri turvallisuudesta vastaaviin tekijöihin organisaation sisällä ja sen ulkopuolella. Erityisen tärkeässä asemassa on lainsäädännön ja erilaisten sopimusten, kuten lisenssisopimusten ja palvelusopimusten vaikutusten arviointi organisaation tietoturvakäytäntöihin. (1.)

Fyysinen turvallisuus

Fyysiseen turvallisuuteen kuuluvat rakennuksen tilojen ja niihin sijoitettujen laitteiden suojaaminen erilaisilta fyysisiltä uhkilta, kuten ilkivallalta ja murroilta, sekä ympäristöuhkilta, kuten vesi- ja palovahingoilta tai sähkö- ja lämmitysjärjestelmien toimintahäiriöiltä. (1.)

Fyysisestä turvallisuudesta vastaa yleensä kiinteistönhuolto ja vartiointi. On tärkeää, että IT-alan henkilöt ovat mukana tilojen suunnittelussa ja laitteiden sijoittelussa, jotta tekniikalle saadaan paras mahdollinen toimintavarmuus. Kameravalvonnan avulla voidaan torjua tietomurtoja, tai pahimmassa tapauksessa selvitellä niitä jälkeenpäin.

Henkilöturvallisuus

Henkilöstöturvallisuuteen kuuluvat ne toimet, joilla sekä varmistetaan tietojärjestelmän käyttäjien toimintakyky että rajataan heidän mahdollisuuksiaan käyttää organisaation tietoja ja tietojärjestelmiä. Näihin toimiin kuuluvat varamiesjärjestelyt, tietojärjestelmiin liittyvän koulutustoiminnan järjestäminen, tietojärjestelmiä koskevien vastuiden ja oikeuksien määrittely sekä erityistapauksissa mahdollisten taustatietojen, esimerkiksi rikosrekisteritietojen, selvittäminen. Henkilöturvallisuudesta vastaa yleensä organisaation henkilöstöhallinto yhdessä tietohallinnon ja muiden turvallisuuselinten kanssa. (1.)

Laitteiden ollessa nykypäivänä pääsääntöisesti suojattu hyvin suurin osa tietoturvariskeistä johtuu henkilöstön tekemistä virheistä. Tämän takia henkilöstölle tulisi suorituttaa tietoturvakoulutus, jossa heille koulutetaan, mikä on sallittua ja mikä ei. Jo rekrytointivaiheessa tulisi vaatia jonkinlaista tietoteknistä osaamista, jos henkilö tulee työskentelemään tilassa, jossa osaamista vaaditaan.

Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen kuuluvat tietojen säilyttämiseen, varmistamiseen ja palauttamiseen sekä tuhoamiseen liittyvät toimet. Aineistoihin kuuluvat myös manuaalisen tietojenkäsittelyn asiakirjat sekä automaattisen tietojenkäsittelyn tulosteet. Tietoaineistoturvallisuudesta vastaa yleensä tietohallinto sekä organisaation arkistoinnista vastuussa oleva yksikkö. (1.)

Tiedot jaetaan organisaatiosta riippuen yleensä neljään eri luokkaan tiedon arkaluonteisuuden mukaan. Nämä luokat ovat:

- erittäin salainen
- salainen
- yhtiönsisäinen
- julkinen (1.).

Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen kuuluvat nimensä mukaisesti ohjelmistoihin liittyvät seikat. Niitä ovat esimerkiksi ohjelmistojen testaus, jolla varmistetaan mm.

- sovellusten sopivuus suunniteltuun käyttötarkoitukseen
- ohjelmistojen keskinäinen yhteensopivuus
- toiminnan luotettavuus ja virheettömyys.

Lisäksi ohjelmistoturvallisuuteen kuuluvat ohjelmistoversioiden ja lisenssien hallinta. (1.)

Ohjelmistoturvallisuuden ylläpito on käytännössä sitä, että huolehditaan ohjelmistojen ja käyttöjärjestelmien säännöllinen päivittäminen. Tämä ehkäisee mahdollisten haavoittuvuuksien tulemisen järjestelmiin. (1.)

Laitteistoturvallisuus

Laitteistoturvallisuuteen liittyvät tietokoneiden ja muiden tietojärjestelmään kytkettyjen laitteiden mitoitus, toiminnan testaus, huollon järjestäminen sekä varautuminen laitteiden kulumiseen ja vanhentumiseen. Laitteistoturvallisuuteen kuuluu myös laitteiden käytöstä aiheutuvien vaaratekijöiden, kuten sähköiskun tai muun loukkaantumisvaaran, välttäminen. (1.)

Laitteistoturvallisuudesta yrityksissä huolehtii yleensä IT-tuki, joka huolehtii viallisten laitteiden huoltamisesta tai vaihtamisesta uuteen. Viallisen koneen käyttäjä on vastuussa siitä, että viat raportoidaan ennen kuin vahinkoja ehtii syntymään.

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen, kuten lähi- ja laajaverkkoyhteyksien sekä muiden viestintäjärjestelmien turvallisuudesta. Tietoliikenneturvallisuus on tärkeä osa tietoturvaa etenkin luottamuksellisuuden kannalta, verkkojen tulisi olla suojattuja ulkopuolisten hyökkäyksien ja tietojen kaappauksen varalta. (1.)

3 Tietoverkot

Tietoverkko on tietoliikenneverkko jonka välityksellä tietokoneet ja muut verkon järjestelmät pystyvät kommunikoimaan keskenään. Tieto siirtyy verkossa paketteina kaapeleita pitkin tai langattomissa verkoissa radioaaltoina.

Tietoverkkoon kuuluvia fyysisiä laitteita voivat olla muun muassa:

- Työasema (workstation) eli käyttäjän henkilökohtainen tietokone.
- Palvelin (server) eli tietokone johon on asennettu palvelinohjelmisto. Palvelin tarjoaa palveluja tietoverkon muille laitteille.
- Reititin (router) eli tietoverkkoja yhdistävä laite, joka välittää tietoja tietoverkon eri osien välillä. Se ohjaa paketteja eteenpäin kohdeosoitteen verkkotunnuksen perusteella.
- Kytkin (switch) eli laite, joka yhdistää paikallisverkon osia. Tunnistaa sen portteihin liitettyjen koneiden MAC-osoitteet ja vie paketit perille niiden perusteella. Kytkimillä on mahdollista myös segmentoida verkko pienempiin osiin.
- Palomuuri (firewall) eli järjestelmä, joka suodattaa yhteyksiä suojattavan ja uhkaavan verkon (yleensä internet) välillä. Laitteena toimii yleensä reititin tai palomuuriohjelmistolla varustettu tietokone.

Tietoverkon tarkoitus on yleensä resurssien ja palveluiden jakaminen käyttäjille. Näitä palveluita voivat olla esimerkiksi internet-sivut, sähköposti, tallennustila ja tulostuspalvelut. Palvelut perustuvat yleensä asiakas-palvelinsuhteeseen; asiakas pyytää palvelimelta tarvitsemaansa palvelua ja palvelin jakaa niitä. Laitteiden välinen keskustelu tapahtuu eri protokollien avulla. (3.)

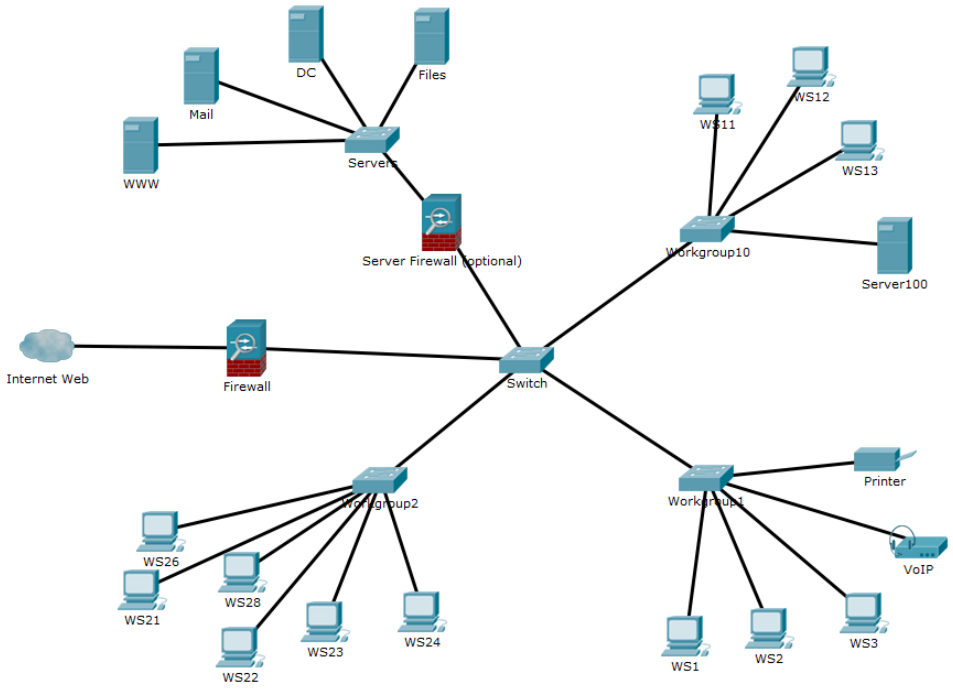
3.1 Tietoverkon rakenne

Tietoverkot jaetaan yleensä käyttötarkoituksen perusteella kahteen ryhmään, jotka ovat vertaisverkot ja palvelinverkot.

Vertaisverkoissa eli P2P- tai workgroup-verkoissa ei käytetä palvelimia, vaan kaikki laitteet ovat työasemia, jotka voivat jakaa toistensa resursseja. Kaukana toisistaan sijaitsevat vertaisverkon koneet voidaan yhdistää toisiinsa internetin ja P2P-

ohjelmistojen avulla. Tätä tekniikkaa käytetään usein myös laittomaan tiedostojen jakamiseen. (5.)

Palvelinverkoiksi kutsutaan verkkoja, joissa on yksi tai useampi laite joihin on asennettu palvelinkäyttöjärjestelmä ja laite tai laitteet jakavat resursseja verkon muille koneille. Verkot voidaan jakaa niiden koon perusteella eri luokkiin, eri luokkia on esimerkiksi LAN (Local Area Network) ja WAN (Wide Area Network). LAN-verkko yhdistää huoneen, talon tai toimipisteen toisiinsa. WAN yhdistää useat LAN-verkot toisiinsa (3.). Kuvassa 1 on esitetty yksinkertainen LAN-verkko.



Kuva 1. Yksinkertainen LAN-verkko.

3.2 OSI-malli

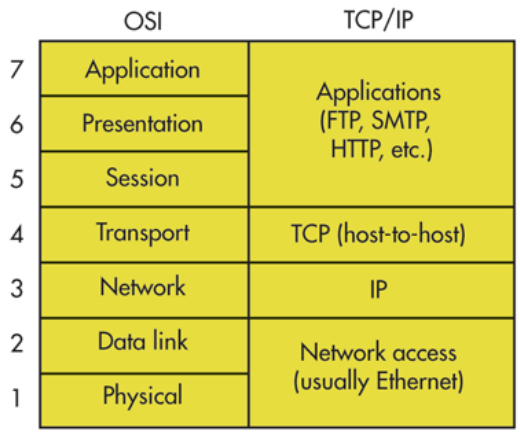
OSI-mallin tarkoitus on yhdenmukaistaa verkkoprotokollajärjestelmiä ja helpottaa erilaisten järjestelmien liittämistä toisiinsa. Se on jaettu seitsemään kerrokseen (kuva 2), joissa kerrosten tehtävät sekä niiden liittymät toisiin kerroksiin on määritelty. (6.)

Kuva 2. OSI-malli (12.).

- Fyysinen kerros huolehtii bittien siirtämisestä fyysisten medioiden välillä. Se tarjoaa fyysisen rakenteen ylemmille kerroksille.
- Siirtokerros huolehtii tiedon luotettavasta siirtämisestä, se tapahtuu kehystämällä paketit fyysisen kerroksen siirtoa varten.
- Verkkokerros huolehtii kehysten tai pakettien reitittämisestä verkon yli. Se ohjaa tietopaketit oikeaan paikkaan osoitteiden avulla.
- Kuljetuskerros tarjoaa pakettien virheettömän kuljetuksen perille asti. Varmistaa että paketit saapuvat perille oikeassa järjestyksessä ja tarvittaessa uudelleenlähettää paketteja.
- Istuntokerros muodostaa ja purkaa yhteyksiä kuljetuskerroksen päälle.
- Esitystapakerros määrittelee ja muuntaa siirron aikana käytettävät esitystavat. Pakkaa datan muotoon, jota sovellukset voivat hyödyntää.
- Sovelluskerros määrittelee tietoliikennesovellukset. Käytännössä toimii rajapintana sovelluksen ja tiedonsiirron välillä sekä muuttaa datan selkokieliseksi käyttäjälle. (7.)

3.3 TCP/IP-protokollaperhe

TCP/IP on protokollaperhe, johon kuuluu TCP- ja IP-protokollien lisäksi myös muita lukuisia protokollia, kuten ARP, UDP, HTTP, FTP ja SMTP. Pääosa näiden protokollien liikennöinnistä tapahtuu TCP-yhteyksinä IP-protokollien päällä. Tästä juontaa juurensa protokollaperheen nimi TCP/IP. TCP/IP-mallilla on paljon yhteistä OSI-mallin kanssa, kuvassa 3 on esitelty mallien keskinäistä suhdetta.



Kuva 3. OSI-malli ja TCP/IP (7.).

Seuraavaksi esitellään muutamia TCP/IP-protokollaperheen protokollia ja palveluja, niiden tehtäviä ja ominaisuuksia.

IP on verkkojen välinen protokolla, joka vastaa pakettien reitittämisestä laitteiden ja IP-verkkojen välillä. IP-prokollasta on käytössä kaksi versiota, IPv4 ja IPv6, joista ensin mainittu on vielä yleisemmässä käytössä.

TCP on UDP:n kaltainen, mutta huomattavasti monipuolisempi kuljetuskerroksen protokolla. Se on yhteydellinen, luotettava, virheenkorjaava ja kuittaava protokolla. TCP:n tiedonsiirto on suunniteltu luotettavaksi ja sen toiminta nojaa siihen, että käytössä on monikerroksinen protokollapino ja että pinon alapuolella oleva verkkokerroksen protokolla pystyy tarjoamaan palvelua paketin välittämiseksi verkossa. TCP on päästä päähän toimiva protokolla, ja kaikki datavälitys tapahtuu lähettävän ja vastaanottavan koneen välillä. Lähettävän ja vastaanottavan koneen välissä voi olla useampiakin TCP -yhteyksiä samanaikaisesti. (8.)

TCP-protokolla käyttää viestinnässä porttinumeroita ja jokaisella TCP:tä käyttävällä ohjelmalla on oma porttinsa. TCP-yhteydet avataan aina ohjelmien välille, joten yhteydet voidaan yksilöidä tarkalleen lähteen ja kohteen IP-osoitteen ja portin avulla. IP-osoitteen ja portin yhdistelmää kutsutaan yhdessä soketiksi. (6.)

UDP on yhteydetön protokolla, joka tarkoittaa sitä, että paketti lähetetään vastaanottajalle, mutta lähetyksestä ei tehdä minkäänlaista ilmoitusta. Myöskään vastaanottaja ei lähetä tietoa siitä, että paketti olisi vastaanotettu. Tämän takia käytössä

ei ole minkäänlaista tiedonvälityksen virheenkorjausta. UDP:n etuna TCP:n nähden voidaan pitää sen kevyempää rakennetta. UDP:tä käytetään sovellusprotokollien, kuten SNMP-verkonhallintaprotokollan, NetBIOS-nimipalvelun ja DNS-nimipalvelun kanssa. (6.)

ARP on protokolla jota käytetään, kun jonkin laitteen tarvitsee selvittää samassa IP-verkossa olevan toisen laitteen fyysisen MAC-osoitteen. Kysely (request) lähetetään broadcastina kaikki aliverkon laitteet kuulevat ARP-kyselyn mutta normaalisti siihen vastaa vain tiedustelua koskevan IP-osoitteen omistava laite. Vastaus lähetetään suoraan kysyjälle request-viestissä tulleeseen MAC-osoitteeseen. Kysyjä tallentaa saadun MAC- ja IP-osoiteparin omaan ARP-tauluunsa. (6.)

ICMP-protokollan tarkoitus on viestiä verkon laitteiden erilaisista ongelmista ja virheistä. ICMP toimii IP-kerroksen päällä, ja paketit lähetetään kohteisiin IP-osoitteiden perusteella. ICMP-pyyntö/vastaus tunnetaan yleisesti myös nimellä ping.

DNS eli nimipalvelu on palvelu, jolla pystytään selvittämään IP-osoitteiden perusteilla niitä vastaavat nimet ja päinvastoin. Nämä tiedot on ympäri maailmaa olevien nimipalvelimien tietokannoissa, joissa on IP-osoitteita ja niitä vastaavia nimiä. (8.)

DHCP-palvelu jakaa IP-osoitteita verkon laitteille. DHCP-palvelua voi tarjota esimerkiksi palvelin tai esimerkiksi reititin. Kun työasema ottaa käynnistyessään yhteyttä verkkoon, sillä ei ole vielä IP-osoitetta. Laite joutuu käyttämään broadcast-lähetystä, jossa se kysyy verkon laitteilta, olisiko niissä jossakin DHCP-palvelua. Jos verkossa on palvelulla varustettu kone, se vastaa kyselyyn ja antaa työasemalle tarvittavat asetukset. (9.)

3.4 Tietoverkkojen tietoturva

Tietoverkkojen yleisimpiä uhkia ovat:

- Erilaiset haittaohjelmat, kuten madot ja troijalaiset. Haittaohjelmia vastaan suojaudutaan virustorjuntaohjelmistoilla.
- Väliintulohyökkäykset, joissa kahden laitteen välistä liikennettä salakuunnellaan ja mahdollisesti muokataan. Hyökkäysmenetelmiä ovat esimerkiksi ARP- ja DNS-väärennökset sekä väärinreititys.

- DNS-kaappaus, jossa murtaudutaan nimipalvelimelle ja laitetaan se lähettämään vääriä osoitteita.

- Palvelunesto- eli DoS-hyökkäykset, jossa pyritään pakottamaan kohde vikatilaan jossa se ei voi tarjota palvelujaan. Hyökkäys voidaan toteuttaa eri tavoin, esimerkiksi tulvittamalla kohde yhteydenmuodostusyrityksillä.

- Social engineering, joka tarkoittaa monimuotoista tiedonkalastelua, jolla hyökkääjä pyrkii saamaan uhrilta salattua tietoa. Tietoja voidaan kalastella esimerkiksi sähköpostilla, puhelimitse tai muulla yhteydenotolla. (3.)

Tietoturvauhkille kehitetään suojausratkaisuja lähes samaa tahtia kuin uhkia ilmenee. Suojausratkaisut voidaan jakaa kolmeen eri menetelmään: kohdesuojaukseen, aluesuojaukseen ja kryptografiisiin menetelmiin. Kohdesuojauksella tarkoitetaan laitekohtaista suojausmenetelmää eli esimerkiksi työaseman virustorjuntaohjelmistojen käyttöä ja käyttöoikeuksien rajoitusta. Aluesuojauksella tarkoitetaan verkon jakamista eri segmentteihin ja alueiden suojaamista tarpeen mukaan palomuureilla. Kryptografisilla menetelmillä pyritään paikkaamaan TCP/IP-mallin turvallisuuspuutteita. Yksi menetelmä on esimerkiksi verkossa liikkuvan tiedon salaaminen salakirjoitusmenetelmillä. Tietoturvasuunnittelu tulisi tehdä eheyttä, käytettävyyttä ja luottamuksellisuutta silmälläpitäen ja niin, että suojattava tieto on suojassa ilman että käytettävyys kärsii liikaa. (3.)

Erityisen tärkeää on palvelinten ja palvelinryhmien tietoturva. Siksi palvelimet olisi hyvä varustaa palomuurilla, jossa vain välttämättömät portit ovat avoinna. Käyttäjätunnusten ja salasanojen tulisi olla vahvoja, sekä hallinnointioikeudet sisältäviä tunnuksia tulisi jakaa mahdollisimman vähän. Uhkien minimoimiseksi olisi hyvä rajoittaa yhteydenotot palvelimille vain tietyn IP-osoitteen omaavalle ryhmälle, esimerkiksi VLAN:ien avulla. Näin mikä tahansa verkon kone ei pääse yrittämään palvelimelle kirjautumista. Palvelimilla on usein käytössä myös kirjautumista rajoittava menetelmä, jossa väärät tunnukset ja salasana voidaan syöttää vain muutaman kerran, jonka jälkeen palvelimelle kirjautuminen lukkiutuu tietyksi määräajaksi. Tällä estetään murtautuminen laitteelle käyttämällä bruteforcea, menetelmää, jossa yritetään arvata käyttäjätunnus ja salasana syöttämällä suuri määrä eri käyttäjätunnus- ja salasanayhdistelmiä koneelle.

4 Penetraatiotestaus

Penetraatiotestaus on verkon testausmenetelmä, jonka tavoite on haavoittuvuuksien ja tietoturva-aukkojen löytäminen. Se on monivaiheinen operaatio, jossa hyökätään kohdeverkkoon. (4.)

Testaus on jaettu yleensä kahteen eri lähtökohtaan. Toisessa on selvitetty etukäteen asiakkaan kanssa testattava verkko ja järjestelmät. Tätä tapaa käytettäessä tiedonkeruu- ja verkonkartoitusvaihetta ei tarvita ja testaus on siten nopeampaa. Toisessa lähtökohdassa testaus tehdään alusta asti eikä asiakas anna mitään tietoja testaajalle, vaan testaaja pyrkii itse hahmottamaan asiakkaan organisaation aina toimipisteiden sijainnista verkkoon ja järjestelmiin asti. (4.)

Tämän ajattelun pohjalta on määritelty kolme eri testaustyyppiä: blackbox, whitebox ja greybox. Blackboxissa testaajalla ei ole mitään tietoja organisaatioista ja sen järjestelmistä. Whiteboxissa testaajalla on käytössään kaikki tieto asiakkaan organisaatiosta ja järjestelmistä. Greybox-testaus on whitebox- ja blackbox-testauksen välimuoto, jossa testaajalle annetaan ennakkotietoja järjestelmästä. Esimerkiksi sisäverkon testauksessa testaajalle voidaan antaa IP-osoitteita ja käyttäjätili testauksia varten. (4.)

Tiedonkeruu

Tiedonkeruuvaiheessa pyritään selvittämään mahdollisimman paljon ennakkotietoja testattavasta kohteesta. Tietojen avulla voidaan päätellä, mitä kautta haluttuihin järjestelmiin päästään käsiksi. Tiedonkeruu voi olla joko passiivista tai aktiivista. (4.)

Passivisella tiedonkeruulla tarkoitetaan menetelmiä, joissa ei olla varsinaisesti kosketuksissa kohteeseen. Passiivista tiedonkeruuta on esimerkiksi julkisesti saatavilla olevan tiedon kerääminen ja analysointi. Tietolähteitä voivat olla esimerkiksi

- sosiaalinen media: facebook, twitter, linkedIn
- yleiset hakukoneet: google, bing
- puhelinluettelot: fonecta, numeropalvelut
- Domain- ja WHOIS-rekisterit: netcraft.com, ripe.net

- DNS-tiedot (Domain Name System): windowsilla nslookup-työkalu, linuxilla dig-työkalu
- yritysrekisterit: finder, Suomen yritysrekisteri
- työpaikkailmoitukset: organisaation verkkosivut, rekrytointipalvelut.

Aktiivista tiedonkeruuta ovat verkkojen skannaaminen sekä menetelmät, joissa vaaditaan ihmisten vuorovaikutusta. Skannaaminen voidaan jakaa kolmeen eri osa-alueeseen: verkko-, portti- ja haavoittuvuusskannaukseen. Esimerkiksi nmap on usein skannauksissa käytetty työkalu. Skannausprosessi voidaan jakaa kolmeen eri vaiheeseen:

- Etsitään verkon laitteet jotka vastaavat eli ovat hengissä.

  Hengissä olevat laitteet voidaan löytää esimerkiksi pingin eli ICMP-kyselyn avulla. Tulosten perusteella tarvittavat toimenpiteet kohdistetaan havaittuihin järjestelmiin.

- Etsitään vastanneiden laitteiden aukinaiset portit.

  Avonaisten porttien löytäminen tapahtuu esimerkiksi TCP ja UDP-kyselypaketteja käyttäen.

- Pyritään tunnistamaan laitteiden käyttöjärjestelmät ja versiot.

  Porttiskannausmenetelmillä voidaan myös selvittää käyttöjärjestelmät ja niiden versiot, tätä kutsutaan OS fingerprintingiksi.

Tietoa kerättäessä ja analysoitaessa tulokset kirjataan muistiin, koska tiedot luovat pohjan seuraaville vaiheille. (4.)

Riskianalyysi

Riskianalyysin tarkoitus on tehdä riskianalyysi edellisten kohtien tietojen perusteella. Se auttaa hahmottamaan kohdeorganisaatio tärkeimpiä suojattavia kohteita ja muita kohteita, joiden kautta voidaan mahdollisesti hyökätä ensisijaisiin kohteisiin. Riskianalyysi on olennainen vaihe lähinnä whitebox–tyyppisessä testauksessa jossa kohdeorganisaatio antaa laajat ennakkotiedot testaajalle. (4.)

Haavoittuvuudet ja hyökkäys

Penetraatiotestauksen tarkoitus on etsiä järjestelmien heikkouksia, joita vastaan voidaan hyökätä. Haavoittuvuus voi johtua esimerkiksi käyttöjärjestelmän ja ohjelmien päivitysten asentamatta jättämisestä tai huonosta verkon konfiguroinnista. Kohdeympäristön palvelimien, käyttöjärjestelmien, porttien ja palveluiden selvittämisen jälkeen voidaan etsiä mahdollisia haavoittuvuuksia. Haavoittuvuuksia voidaan etsiä hyödyntäen internetissä olevia haavoittuvuustietokantoja. (3.)

Haavoittuvuuksien etsimistä varten on olemassa myös erilaisia haavoittuvuus-skannereita, kuten Metasploit ja OpenVAS. Nämä ovat ohjelmia, jotka on suunniteltu etsimään haavoittuvuuksia järjestelmistä, verkosta ja sovelluksista. Ohjelmat lähettävät testattavalle kohteelle kyselyitä ja analysoivat saamansa vastauksen. Vastaanotetun tiedon perusteella määritellään esimerkiksi versio ja päivitysten tilanne. Vastauksia verrataan haavoittuvuustietokantaan, jonka jälkeen ohjelma muodostaa raportin löytyneistä haavoittuvuuksista. (3.)

Haavoittuvuuksien skannauksessa on huomioitava, että IDS/IPS-järjestelmät pyrkivät havaitsemaan juuri tämän tyyppistä toimintaa. Penetraatiotestaaja pyrkii jäljittelemään oikeaa hyökkäystä mahdollisimman tarkasti, joten hän myös pyrkii välttämään toimintansa havaitsemisen. Havaitsemista voidaan vaikeuttaa tekemällä skannaukset hitaasti ja pienissä osissa. Tämä luonnollisesti vaatii paljon aikaa, jota oikeassa hyökkäystilanteessa harvoin on saatavilla. (3.)

Hyökkäysvaiheessa tunkeudutaan järjestelmiin, joista on löydetty haavoittuvuuksia edellisten testausvaiheiden aikana. Hyökkäystä tehdessä tulee olla varovainen ja ottaa huomioon kohteen mahdolliset vastatoimet. Puolustustoimia ovat IDS/IPS-järjestelmien lisäksi muun muassa virustorjuntaohjelmistot ja palomuurit, joiden on tarkoitus estää verkon ja laitteiden luvaton käyttö. Hyökkääjän tavoitteena on tunkeutua järjestelmiin kiertäen nämä edellä mainitut turvatoimet. (4.)

Väliintulohyökkäys on nimensä mukaisesti hyökkäys, joka tehdään kahden järjestelmän välissä. Liikenne kulkee hyökkääjän järjestelmän kautta uhrin kuvitellessa liikenteen kulkevan yhä suoraan kohteeseen. Tavoitteena hyökkäyksessä on kaapata verkkoliikennettä analysoitavaksi tai muokata sen sisältöä. Hyökkäys vaatii pääsyn

paikalliseen lähiverkkoon. Erilaisia väliintulohyökkäystekniikoita on esimerkiksi ARP-poisoning, DNS-spoofing ja DHCP-spoofing. (5.)

Jälkihyökkäys

Jälkihyökkäysvaiheessa tarkastellaan saatujen tietojen arvo, arvioidaan kuinka onnistunut hyökkäys oli ja selvitetään, päästäisiinkö käytettyä hyökkäysreittiä pitkin vielä syvemmälle kohteen järjestelmiin. Testaaja voi vielä tarpeen mukaan piilottaa järjestelmään takaportin, jonka avulla päästään takaisin sisälle. (4.)

5 Tietoturvakartoitus yritykselle

5.1 Lähtökohdat

Tietoturvatestauksen alkuperäisenä lähtökohtana oli tehdä yritykselle verkon penetraatiotestaus ulkoapäin ja kartoittaa tietoturvan tasoa eri osa-alueilta. Ensimmäisessä yritystapaamisessa sovittiin, että testauksissa keskitytään neljään eri kohteeseen:

- sisäverkon testaus sisältäpäin
- ulkoverkon testaus ulkoapäin
- työasemien tietoturva
- Web-portaalin tietoturva.

Insinöörityössä keskitytään ainoastaan sisäverkon testaukseen ja työasemien tietoturvaan testauskohteiden laajuuden ja ajan puutteen takia. Yritystapaamisessa (16.) saatiin ennakkotietoja testausta varten, näitä tietoja on kuvattu taulukoissa 1 ja 2. Kaikki IP-osoitteet on muutettu tätä raporttia varten.

Taulukko 1. Sisäverkon testauksen lähtökohdat

Sisäverkon testauksen lähtökohdat	
Verkkoalue	- 10.100.0.0/14 - Osoitteet 10.100.0.0-10.103.255.255
Laitteet	- 2000 työasemaa ja 350 palvelinta. - Lukuisia toimipisteitä ympäri Suomea ja Eurooppaa. - Lähiverkkoon kytkimillä autentikointi osalla kytkimistä, suurimmalla osalla ei käytössä. - Työasemista suurin osa samalla Windows 7 imagella. - Palvelimet mm. Windows Server 2008, myös Server 2003 -laitteita löytyy.
Testaus	- Työkaluna voi käyttää Nmapia ja Wiresharkia.

Taulukko 2. Työasemien tietoturva

Työasemien tietoturvan lähtökohdat	
Virustorjunta	- McAfee Antivirus -virustorjunta ohjelmistot ja yrityksen oma Firewall. - Sähköpostissa kaksinkertainen suodatus sekä kolminkertainen virtustarkistus.
Käyttäjätunnukset	- Windows salasanat täytyy vaihtaa 48 päivän välein. - Minimipituus 8 merkkiä ja kolmea edellistä käytössä ollutta salasanaa ei voi käyttää. - Käyttäjätunnukset yrityksen domainissa ja tunnukset ovat muotoa etunimi.sukunimi. - Sovelluksiin erilliset tunnukset.
Rajoitukset	- Internetin käyttöä rajoitetaan paljon, tiukka proxy/webfilter.
Testaus	- Mitä kadonneella koneella voidaan tehdä? - Mitä tehdä kun laite katoaa? Prosessin tarkastelu ja parannusehdotuksia.

Yritystapaamisista saatiin paljon tietoa yrityksen tietoturvasta yleisellä tasolla ja mahdollisia puutteita:

- Pääkaupunkiseudulla on kaksi konesalia ja kolmas on tulossa hätätilanteita varten.
- Käytössä viisi WLAN-verkkoa ja yrityksen työasemilla on varmenteet, joilla pääsee verkkoon ilman käyttäjätunnuksia. Osalla on suojaus PSK:lla ja MAC-suodattimella. Avoimia WLAN-verkkoja ei ole lainkaan.
- Yrityksellä on kymmeniä työpisteitä Suomessa, Euroopassa, Aasiassa ja Pohjois-Amerikassa.
- Tiettyjen toimipisteiden valvonta eli fyysinen tietoturva on suurin kysymysmerkki. Tämä oli pohjana sisäverkon testauksille, joiden tarkoituksena oli selvittää mitä voidaan tehdä jos hyökkääjä pääsee vapaasti sisälle toimipisteeseen ja kytkee koneensa kiinni verkkoon.
- Uusille työntekijöille ei järjestetä tietoturvakoulutusta. Alussa kuitenkin täytyy lukea ja allekirjoittaa tietoturvaohjeistus.

5.2 Suunnittelu

Saatujen tietojen perusteella alettiin suunnitella itse testausta. Testauksen tarkoituksena on hahmottaa sisäverkon rakenne skannauksien avulla ja tehdä tarkempia skannauksia laitteille, joilta haavoittuvuuksia yritettiin löytää. Käytännössä testauskone kytketään

verkkokaapelilla kiinni neuvotteluhuoneen kytkimeen. Tarkoituksena on testata, mitä pystytään tekemään, jos tällainen mahdollisuus avautuu hyökkääjälle. Haavoittuvuuksien hyväksikäyttöä ei toteuteta yrityksen laitteisiin vaan niitä voidaan yrittää simuloida omassa virtuaaliympäristössä mahdollisuuksien mukaan. Mikäli laitteista löydetään haavoittuvuuksia, niistä tehdään yritykselle raportti ja kehitysehdotuksia.

Toinen testauskohde on yrityksen käytössä oleva työasema, johon yritetään murtautua ja kaivaa tietoja. Tavoitteena on tutkia mitä varastetulla koneella voidaan tehdä ja pohtia onko mahdollista saada käyttäjätunnuksia haltuun esimerkiksi social engineeringillä. Social engineeringiä pohditaan teoreettisellä tasolla eikä sitä toteuteta käytännössä, ajan puutteen takia. Lisäksi selvitetään minkälainen prosessi yrityksellä on käytössä tällaisten tilanteiden varalle ja miten sitä voitaisiin kehittää. Tutkimuksen tulosten perusteella yritykselle raportoidaan nykyisten toimintamallien mahdollisista puutteista. Kaikki sisäiset testaukset suorittiin yrityksessä työskentelevän IT-henkilön valvonnassa ja testaussuunnitelmat toimitettiin hänelle etukäteen.

5.3 Työkalut

Testauskoneena käytettiin peruskannettavaa jossa oli Windows 8 -käyttöjärjestelmä sekä Nmap- ja Wireshark-ohjelmistot. Muita työkaluja käytännössä tapahtuvassa testausvaiheessa ei ollut lupa käyttää. Haavoittuvuuksia voidaan myös etsiä jälkeenpäin ja tutkia teoreettisia mahdollisuuksia hyödyntää niitä. Tähän käytettiin Kali Linuxia, penetraatiotestausta varten kehitettyä käyttöjärjestelmää, joka sisältää lukuisia tunnettuja penetraatiotestaustyökaluja.

Nmap

Nmap on ehkä kaikkein suosituin porttiskannaustyökalu, jonka ensimmäinen versio julkaistiin vuonna 1997. Nmap on ilmainen komentopohjainen työkalu, josta on saatavilla myös graafinen versio Zenmap. Työkalulla pystytään skannaamaan verkossa olevia laitteita lähettämällä näille eri paketteja, kuten esimerkiksi yleisimmät ICMP, TCP SYN ja TCP ACK. Vastausten perusteella voidaan selvittää tavoitettavissa olevien laitteiden avoimet portit, palveluiden versiot, laitteen käyttöjärjestelmä ja sen versio sekä reitti (6.).

Kuvassa 4 on esitetty Zenmapilla tehdyn porttiskannauksen tuloksia. Nähtävissä ovat muun muassa avoimet portit ja laitteen käyttöjärjestelmä.

```
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows
2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:A7:FA:A1 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or
SP2
```

Kuva 4. Zenmap-skannauksen tuloksia.

Wireshark

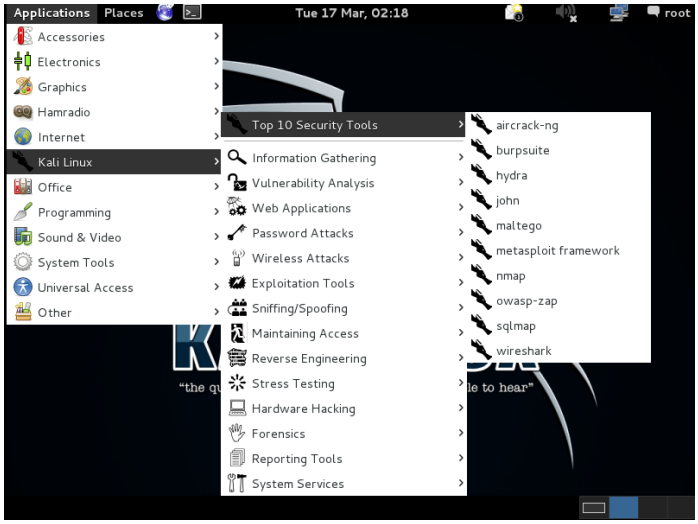
Wireshark on vuonna 2006 ensimmäisen kerran julkaistu verkon analysointiin tarkoitettu avoimen lähdekoodin ohjelmisto. Wireshark monitoroi verkon liikennettä ja pystyy suodattamaan tietoja protokollien mukaan. Kuvassa 5 on esimerkki siitä, minkälaista tietoa Wiresharkilla saadaan.

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	Buffalo_[redacted]	Broadcast	ARP	60	Who has 192.16
2	1.000104000	Buffalo_[redacted]	Broadcast	ARP	60	Who has 192.16
3	1.620506000	192.168.11.2	192.241.[redacted]	TCP	60	60472 > 6851
4	1.741500000	192.168.11.2	171.97.[redacted]	TCP	60	60453 > 6851
5	1.799282000	192.241.[redacted]	192.168.11.2	TCP	66	6851 > 60472
6	2.000136000	Buffalo_[redacted]	Broadcast	ARP	60	Who has 192.16
7	2.021006000	171.97.[redacted]	192.168.11.2	TCP	60	6851 > 60453
8	3.001175000	Buffalo_[redacted]	Broadcast	ARP	60	Who has 192.16
9	4.001281000	Buffalo_[redacted]	Broadcast	ARP	60	Who has 192.16
10	4.022446000	192.168.47.128	192.168.47.2	DNS	85	Standard query

Kuva 5. Wireshark-liikennettä.

Kali Linux

Kali Linux on Debian-pohjainen Linux-jakelupaketti, joka on suunniteltu erityisesti penetraatiotestausta varten. Se sisältää lukuisia tunnettuja testausohjelmia, kuten Nmap, Wireshark, John the Ripper, Aircrack-ng ja Metasploit (12.). Kuvassa 6 on kuvattu Kali Linuxista löytyviä työkaluja.



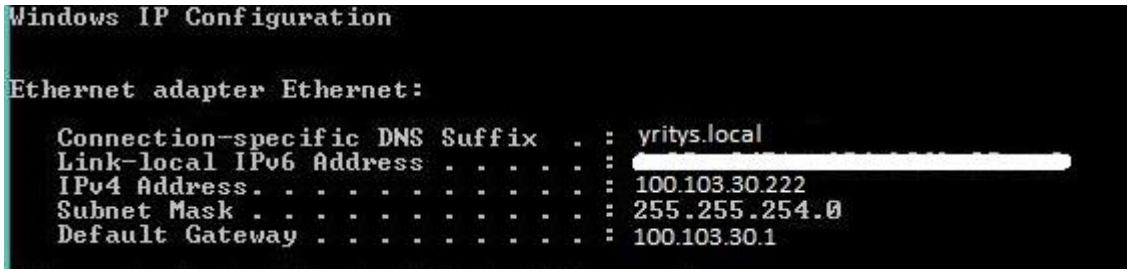
Kuva 6. Näkymä Kali Linuxin työpöydältä.

5.4 Testaus

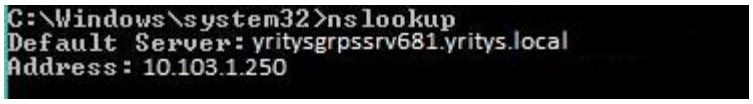
5.4.1 Sisäverkon testaus

Testaus aloitettiin kytkemällä testauskone yrityksen erään toimipisteen neuvottelutilan verkkoon verkkokaapelilla. Kaapelin kytkemisen jälkeen saatiin heti internet-yhteys, joten kytkimillä ei ollut käytössä todennusta tässä tilassa.

Seuraavaksi syötettiin komentoriville peruskomennot ipconfig ja nslookup. Komennolla ipconfig saadaan selville perustietoja joita on esitetty kuvassa 7. Nslookup-komennolla saatiin selville nimipalvelimen IP-osoite ja palvelimen nimi (kuva 8).



Kuva 7. Ipconfig

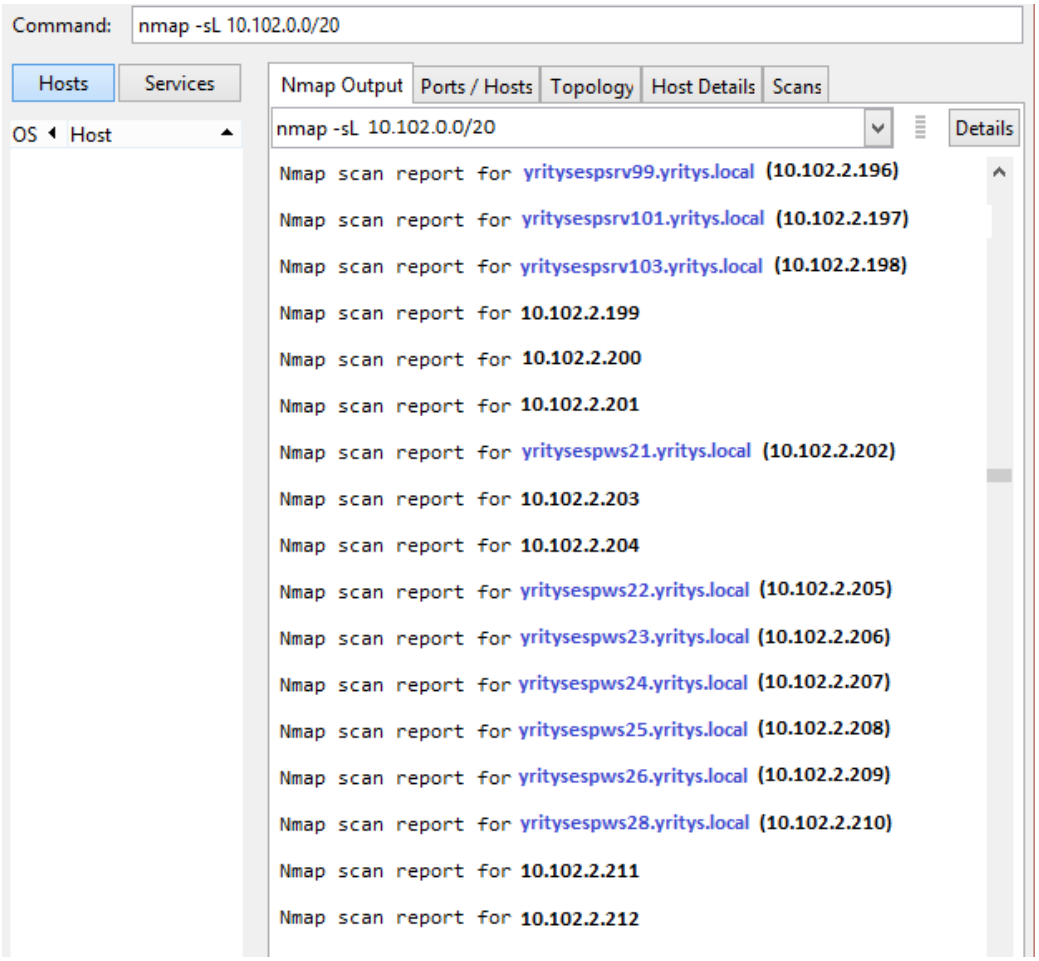


Kuva 8. Nslookup

Wireshark-monitoroinnissa nähtiin enimmäkseen IPv6-protokollan broadcast-paketteja eri laitteiden välillä. Lisäksi havaittiin joitain ARP- ja DHCP-pyyntöjä, joiden avulla olisi mahdollista tehdä Man in the middle -hyökkäyksiä. Sitä ei kuitenkaan tässä testauksessa tehty. Kytkimiltä nähtiin myös STP-viestejä, jotka olivat protokollaa Rapid-Per-VLAN Spanning tree (RPVST). Näitä viestejä olisi mahdollista hyödyntää verkkotopologian selvittämisessä, jos verkkoa testattaisiin eri paikoista. Siihen ei tässä testauksessa keskitytty, koska työ tehtiin kokonaisuudessaan yhdessä paikassa.

Kytkimen hallintaan yritettiin päästä kiinni yrityksen antamalla hallinta IP-osoitteella. Sille ei kuitenkaan päästy kirjautumaan, koska se oli suojattu käyttäjätunnuksella ja salasanalla. Myös kytkimen konsoliyhteys on suojattu tunnuksilla, joten kytkimiä on tässä tapauksessa hankala päästä hallinnoimaan ilman etukäteen hankittuja tunnuksia.

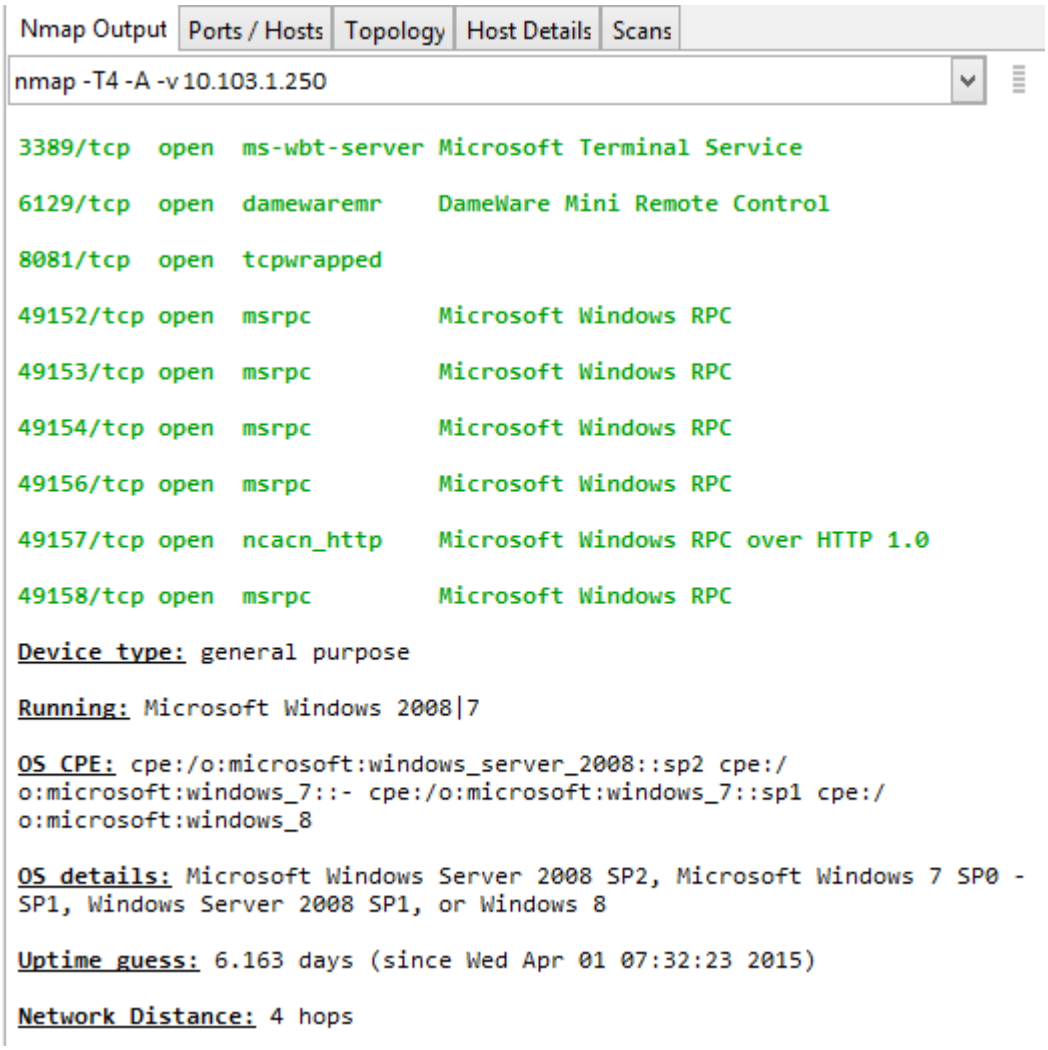
Testausta varten saatiin yritykseltä ennakkotietona IP-osoitealue 10.100.0.0/14. Verkon rakenteen kartoittaminen aloitettiin tekemällä Nmap:lla list scan -skannauksia, jolla selvitetään verkon laitteiden nimet käänteisnimipalvelulla. Laitteiden nimilistauksilla pystytään selvittämään helposti verkon rakennetta, mikäli laitteet on nimetty loogisesti. Kuvassa 9 on esitetty miltä list scan -skannaukset voivat näyttää.



Kuva 9. Nmapin –sL-skannaus.

Kuten kuvastakin voidaan nähdä, yrityksen koneet ja palvelimet oli nimetty rakenteella yrityksen nimi, toimipiste ja laitteen tyyppi. Nimien perusteella pystyttiin hahmottamaan verkon rakennetta aika tarkasti. Tietojen perusteella selvitettiin, että yrityksellä on kymmeniä toimipisteitä ympäri Suomea ja Eurooppaa, ja että toimipisteiden paikalliset verkot muodostuvat yleensä työasemista ja usein myös yhdestä tai useammasta paikallisesta palvelimesta. Toimipisteiden paikallisten verkkojen lisäksi löydettiin kaksi hieman erilaista verkkoaluetta. Toisella näistä alueista kaikki laitteet näyttivät nimien perusteella olevan palvelimia ja toisella alueella vaikeammin tunnistettavia laitteita, joista osasta löytyi kirjainyhdistelmä SAP. Nämä kaksi verkkoa sisältävät keskitetyt palvelut eli konesali- ja tuotannonohjausjärjestelmät.

Näiden tietojen perusteella päätettiin keskittyä lähinnä konesalin palvelimien tarkempiin skannauksiin. Lisäksi skannattiin verkkoalue, jossa laitteet olivat enimmäkseen työasemia. Tarkemmat skannaukset tehtiin Zenmapin intense scan -profiililla, joka etsii laitteen avoimet portit, selvittää käyttöjärjestelmän ja jäljittää reitin laitteelle.

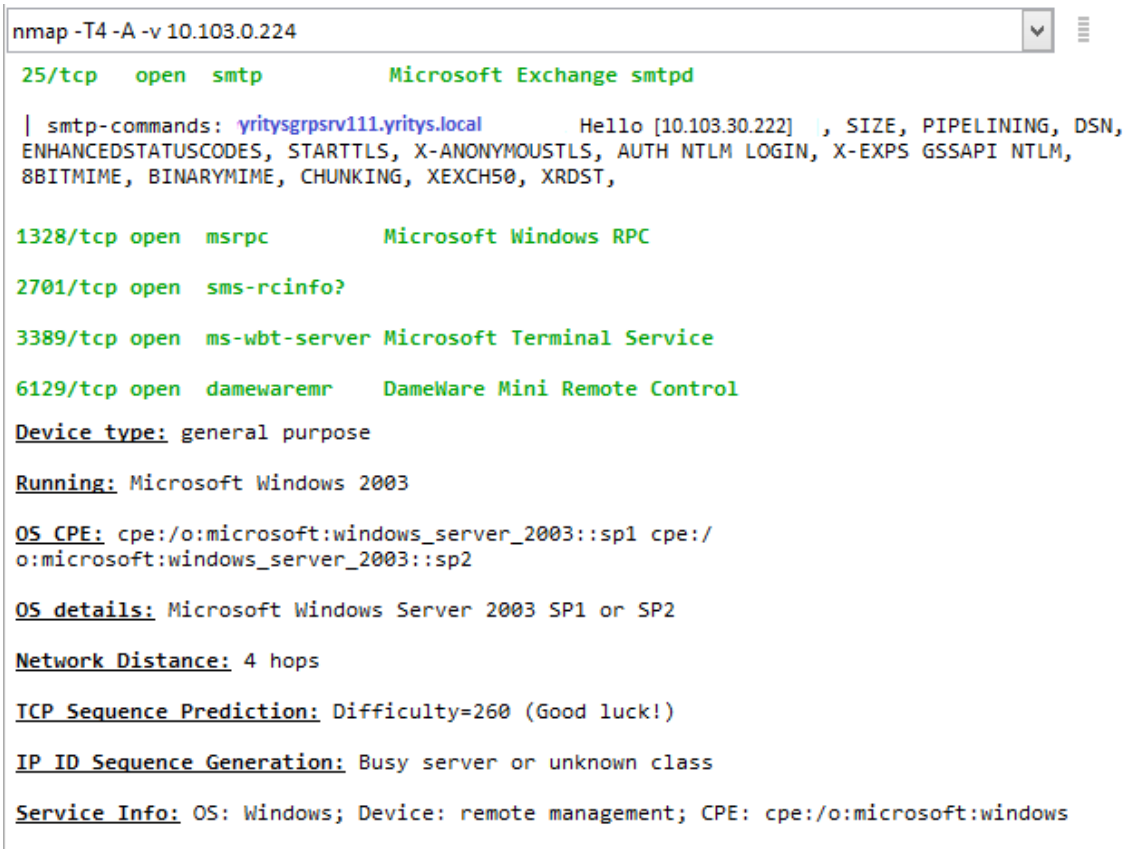


Kuva 10. Intense scan nimipalvelimelle.

Esimerkkiskannaus tehtiin konesaliverkkoon kuuluvalle nimipalvelimelle, jonka IP-osoite selvitettiin myös jo aiemmin nslookupilla. Tuloksista selviää, että laitteen käyttöjärjestelmä on Windows Server 2008 ja siinä on useita portteja avoinna. Palvelimen ja testauskoneen välillä ei ole palomuurisuojausta. Testauskoneella otettiin Windowsin remote desktopilla yhteys palvelimen avoimeen porttiin 3389. Yhteys palvelimeen saatiin luotua, mutta kirjautumista varten tarvittaisiin IT-henkilöstön käyttäjätunnukset. Tätä kautta olisi teoriassa mahdollista päästä kirjautumaan

palvelimelle esimerkiksi bruteforcella tai käyttäjätunnuksilla, jos ne onnistuttaisiin hankkimaan etukäteen social engineering -menetelmillä.

Yrityksellä on käytössä myös Windows Server 2003 -palvelinohjelmistolla varustettuja koneita. Ohjelmiston päivitykset ja tuki on päättymässä näillä näkymin 14.7.2015. Tällainen kone löytyi myös konesaliverkosta, ja sille tehtiin Zenmapilla intense scan -skannaus. (Kuva 11)



Kuva 11. Windows Server 2003 -palvelimen tuloksia.

Myös kuvan 11 palvelimesta löytyi avoin portti etäyhteyksille, ja siihen voidaan ottaa yhteys remote desktopilla. Lisäksi löydettiin avoin SMTP-portti 25, jonka kautta yritettiin muodostaa telnet-yhteys palvelimeen. Testikoneella saatiinkin suora telnet-yhteys palvelimeen ilman todennusta. Samankaltaisia skannaustuloksia saatiin myös eräälle Alankomaista poimitulle Windows Server 2003 -palvelimelle.

Tarkempia skannauksia tehtiin myös yhdelle enimmäkseen työasemia sisältäneelle osoitealueelle. Tuloksista nähtiin että kaikissa työasemissa on asennettuna Windows 7 -käyttöjärjestelmä, joissa suunnilleen samat portit avoinna ja ylimääräisiä , mahdollisesti haavoittuvaisia ohjelmistoja ei havaittu suurimmalla osalla koneista. Sama tilanne oli myös yhdellä, nimen perusteella Ranskassa sijainneella koneella. Tämä johtuu siitä, että yrityksen koneet asennetaan samalta yrityksen imagelta eikä ylimääräisiä ohjelmistoja saa asentaa koneisiin. Ainoa haavoittuvuus, joka löydettiin kahdelta koneelta, oli portissa 80 avoinna ollut Apache Http server-ohjelmiston vanhentuneella versiolla 2.0.44. Kyseessä on versio, jolta on löydetty useita haavoittuvuuksia (15.). Uusin ohjelmiston versio on 2.4.12, ja se olisi suositeltavaa päivittää uudempaan.

Tuotannonohjausjärjestelmään pääsyä yritettiin kirjoittamalla sopivan nimisen laitteen IP-osoite selaimeen. Selaimeen aukesi virtuaalialustan kirjautumisruutu, jolla pääsisi tunnuksilla kirjautumaan hallintajärjestelmään.

5.4.2 Työaseman testaus

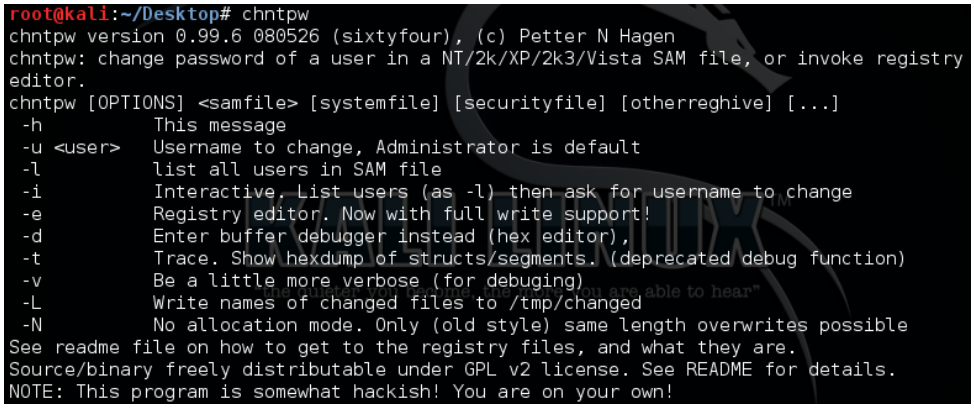
Työaseman tietoturvaa testattiin Kali Linux USB medialla. Käyttöön saatiin yrityksen HP-merkkinen peruskannettava ja tarkoituksena oli testata, miten ja miksi hyökkääjä voisi sitä hyödyntää.

Ensimmäisenä kone käynnistettiin normaalisti käyttöjärjestelmään ja tutkittiin mahdollisuuksia tätä kautta. Windows-kirjautumisruudussa näkyi edellisen koneelle kirjautuneen käyttäjän tunnus, joka oli muotoa etunimi.sukunimi. Käyttäjän nimellä voitaisiin alkaa selvittämään muita käyttäjän tietoja, kuten puhelinnumero ja osoitetiedot. Puhelinsoitolla voitaisiin jossain tapauksessa saada jo suoraan salasana, jos esiinnyttäisiin IT-tukihenkilönä ja ilmoitettaisiin käyttäjälle että tunnuksia tarvittaisiin.

Seuraavaksi yritettiin käynnistää kone Kali Linux USB medialta. Koneen BIOS ei ollut salasanasuojattu, joten boot-järjestys pystyttiin muuttamaan sopivaksi ilman ongelmia. Myöskään secure boot ei ollut koneella oletuksena päällä, joten sitä ei tarvinnut muuttaa. Kone käynnistyi nyt normaalisti Kali Linux -käyttöjärjestelmään, joten salasanan murtaminen voitiin aloittaa.

Ennen salasanan murtamisyrityksiä on järkevää tarkastaa, mitä tietoja koneen kovalevylle on tallennettu. Levyä päästään tutkimaan käyttöjärjestelmän työpöydän kautta ja sieltä kannattaa tarkastaa käyttäjän tiedostot. Parhaassa tapauksessa kansioista saattaa löytyä tiedosto, johon on tallennettu käyttäjätunnuksia ja salasanoja. Tästä koneesta sellaista ei löytynyt. Tässä vaiheessa on myös mahdollista kopioida salasanatiivisteet, murtaa salasana erikseen ja jatkaa hyökkäystä myöhemmin.

Salasanan murtamista yritettiin Kali Linuxin CHNTPW-työkalulla, jonka toimintoja on esitelty kuvassa 12.



Kuva 12. CHNTPW-työkalun näkymä.

Testauksessa yritettiin nollata Administratorin salasanaa komentorivin komennoilla:

- *cd /media/levynimi/Windows/System32/config*
- *chntpw –u Administrator SAM*
- Valitaan *1 - Clear (blank) user password.*

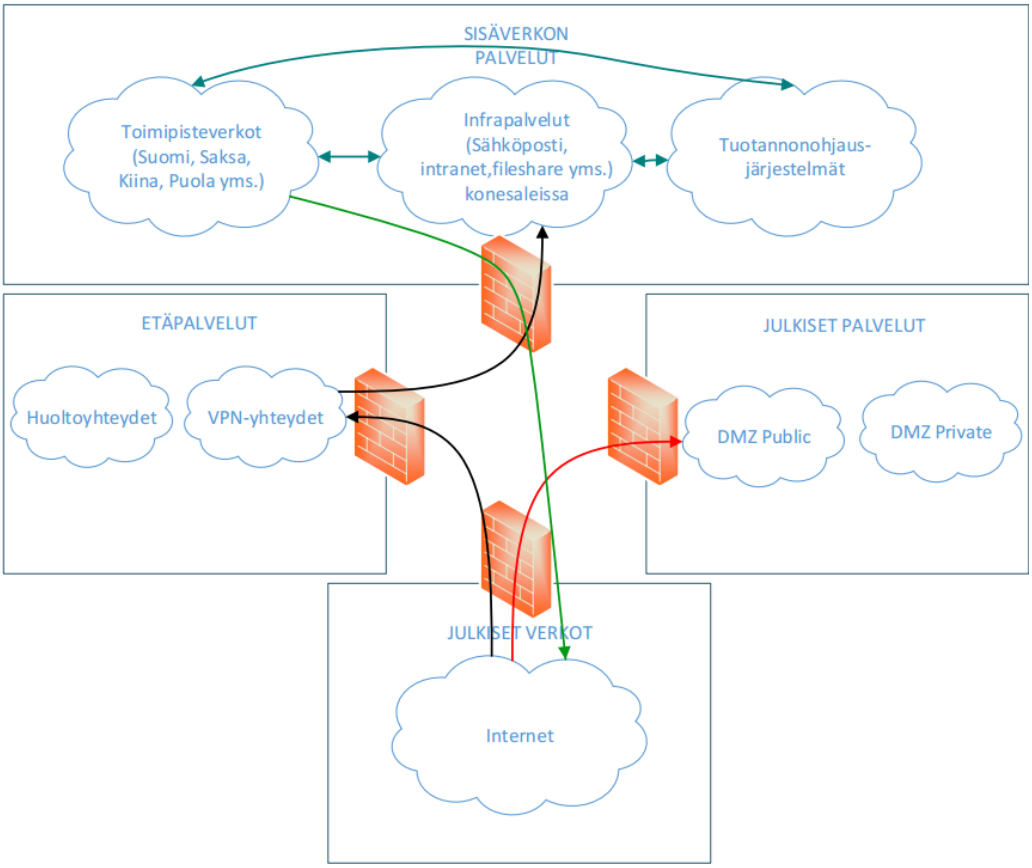
Salasanan nollaus ei kuitenkaan jostain syystä onnistunut näillä komennoilla yrityksen koneelle. Internetistä löytyneiden tietojen mukaan käytetyssä chntpw:n versiossa 0.99.6 on ollut luotettavuusongelmia ja siitä tulisi käyttää versioa 0.99.5. (14) Kali Linuxilla on useita muita salasanojen murtamiseen tarkoitettuja työkaluja, kuten Ophcrack ja John the Ripper. Niitä ei kuitenkaan testattu tässä vaiheessa, vaan siirryttiin eteenpäin vaiheeseen, jossa ollaan päästy kirjautumaan työasemalle administrator-tunnuksilla. (13.)

Työasemalle kirjautumisen jälkeen etsittiin sovelluksia, joita voitaisiin hyödyntää hyökkäyksessä. Tärkeisiin sovelluksiin ei päästy kirjautumaan administrator-tunnuksilla, vaan niihin tarvitaan joko erilliset käyttäjätunnukset tai domain-tunnukset.

Yrityksen koneissa on olemassa varmenteet, joilla pystytään kirjautumaan yrityksen sisäisiin suojattuihin WLAN-verkkoihin ilman käyttäjätunnuksia, kunhan verkolle ensin luodaan profiili. WLAN-verkon kautta päästään myös muuhun yrityksen sisäiseen verkkoon kiinni, joten myös tätä kautta on mahdollista toteuttaa hyökkäyksiä esimerkiksi konesalin laitteisiin tai tuotannonohjausjärjestelmiin.

5.5 Tulokset

Testaustulosten käsittelyä varten saatiin kuva (kuva 13) yrityksen verkosta. Kuvassa on esitetty verkon rakenne kokonaisuutena ja tietoliikenne rajoituksineen eri verkkoalueiden välillä.



Kuva 13. Yrityksen verkko

Kuvasta nähdään, että kaikilta toimipisteiltä on sisäverkon kautta suora pääsy keskitettyihin palveluihin eli infrastruktuuripalveluihin ja tuotannonohjausjärjestelmiin. Tämä tarkoittaa sitä, että esimerkiksi Liettuasta sijaitsevalta toimipisteeltä voidaan yrittää päästä sisälle konesalin palvelimiin remote desktopia käyttämällä. Tähän voisi esittää parannusehdotuksen, jossa palomuuri rajoittaa infrastruktuuripalveluihin ja tuotannonohjausjärjestelmiin tulevaa liikennettä sisäverkosta. Tässä tulee esiin tietoturvan ja käytettävyyden vastakkainasettelu, joten käytännön ratkaisut täytyy suunnitella tarkkaan. Muilta osin verkon rakenne näyttää hyvältä ja ulkopuoliset uhkat, kuten huolto- ja VPN-yhteydet sekä internet on suojattu palomuurein.

Yrityksen tietoturvan nähtiin olevan hyvässä kunnossa yleisellä tasolla. Työasemille täytyy syöttää vahvat salasanat, ja ne täytyy vaihtaa säännöllisesti, laitteiden suojaukset on kunnossa ja internetin käyttöä rajoitetaan paljon.

Yrityksen yleisen tietoturvan ennakkotietoihin perustuvia puutteita olivat

- tiettyjen toimipisteiden fyysinen tietoturva
- työntekijöiden tietoturvakoulutus.

Eri toimipisteiden fyysistä tietoturvaa ei päästy tutkimaan ajan puutteen vuoksi. Kaikki testaukset tehtiin yhdessä toimipisteessä, jossa kulunvalvonta näytti olevan hyvällä tasolla. Aulassa oli jatkuvasti henkilökuntaa valvomassa ja toimistotiloihin pääsi vain henkilökohtaisella kulkutunnisteella. Kaikilla toimipisteillä kulunvalvonta tulisi olla vähintään tällä tasolla ja lisäksi olisi hyvä olla kameravalvonta. Hyvällä fyysisellä tietoturvalla voidaan välttää riskejä, joita sisäverkon ja työaseman tietoturvatestauksissa todettiin.

Työntekijöille ei järjestetä tällä hetkellä lainkaan tietoturvakoulutusta. Käytössä on tietoturvaohjeistus, joka uusien työntekijöiden täytyy lukea ja allekirjoittaa. Tätä osa-aluetta voitaisiin parantaa ottamalla käyttöön esimerkiksi interaktiivinen verkkokurssi, jossa käsiteltäisiin tietoturvan eri osa-alueita työntekijän näkökulmasta. Kurssin tarkoitus olisi antaa käyttäjälle kuva, mikä on sallittua ja mikä ei. Tällaisella pienellä muutoksella saataisiin parannettua tietoturvaa helposti.

Sisäverkon ja kannettavan tietoturvatestauksissa löydettiin seuraavat uhkat:

- Testauskoneella pääsee suoraan internetiin, kun kiinnittää verkkokaapelin.
- Windows Server 2003 -palvelimilla SMTP ei todenna käyttäjiä mitenkään.
- Sisäverkon infrapalveluilla ja tuotannonohjausjärjestelmillä ei palomuuri-suojausta.
- Osalla työasemista käytössä Apache HTTPd-ohjelmiston todella vanha versio.
- Työasemien käyttäjätunnukset ovat muotoa etunimi.sukunimi.
- Työasemien BIOS ei ole salasanasuojattu ja secure boot oletuksena pois päältä.
- Työasemilla on WLAN-varmenne, jolla pääsee sisäverkkoon ilman käyttäjä-tunnuksia.

Windows Server 2003 –palvelimien tuki ja päivitykset päättyy kesällä 2015, joten sitä käyttävien laitteiden käyttöjärjestelmät pitäisi päivittää uudempiin pian. Myös työasemilta löytyneet vanhentuneet Apache-ohjelmistot tulisi päivittää uudempiin.

Työasemien käyttäjätunnusten muotoa voisi miettiä uudelleen, etunimi.sukunimi-muoto antaa liikaa tietoa laitteen käyttäjästä. Nimen perusteella voidaan helposti selvittää käyttäjän puhelinnumero, osoite ja mahdollisesti muita tietoja esimerkiksi sosiaalisesta mediasta. Selvitettyjen tietojen perusteella voidaan lähestyä työaseman käyttäjää ja hankkia tältä yrityksen tietoja.

Laitteiden varastamista voitaisiin välttää ohjeistamalla käyttäjiä pitämään laitteet lukittuina työpisteisiin, jos ne eivät ole käyttäjän valvonnassa. Työasemien tietoturvaa vahvistaisi osaltaan myös BIOSin salasanasuojaus ja secure bootin ottaminen käyttöön. Nämä suojaukset vaikeuttavat ja hidastavat koneen hyväksikäytön aloittamista.

WLAN-varmenne helpottaa käyttäjien langattomaan verkkoon pääsyä. Se tuo mukanaan kuitenkin myös tietoturvariskin, jos käyttäjä osaa hyödyntää sitä ja tietää että langattoman verkon kautta pääsee käsiksi muuhun sisäverkkoon. Tästä johtuen hyökkääjän ei tarvitse välttämättä olla fyysisesti yrityksen tiloissa suorittamassa hyökkäystä, vaan se voidaan tehdä ulkopuolelta langattoman verkon alueella.

Yrityksen prosessi työasemien katoamisen varalle on, että käyttäjä ilmoittaa IT-tukeen laitteen katoamisesta, jonka jälkeen suljetaan käyttäjän käyttäjätili ja poistetaan koneen WLAN-sertifikaatin oikeudet langattomaan verkkoon. Prosessi on tehokas torjumaan tietoturvauhkia, jos käyttäjä havaitsee työaseman katoamisen heti. Jos työaseman katoamista ei huomata, riski on vakava ja sen takia laitteiden katoamisen mahdollisuus tulisi minimoida hyvällä fyysisellä tietoturvalla.

6 Yhteenveto

Insinöörityö keskittyi yrityksen tietoturvaan, ja sen tarkoituksena oli kartoittaa yrityksen tietoturvan yleinen taso sekä sisäverkon- ja työasemien tietoturva. Tietoturvakartoituksen pohjalta oli tarkoituksena pohtia parannusehdotuksia yrityksen tietoturvaan liittyen.

Teoriapohjana työlle oli tietoturvan yleiset lähtökohdat, tietoverkkojen rakenteet ja niiden merkitys yrityksessä sekä penetraatiotestaus osana tietoturvatestausta. Teorian aiheiden rajauksessa onnistuttiin mielestäni hyvin, ja se antoi pohjan testauksille. Periaatteessa etenkin penetraatiotestauksen menetelmiin olisi voinut mennä syvemmällekkin, mutta näillä resursseilla ja aikataululla se ei olisi ollut järkevää.

Yrityksen tietoturvan yleisen tason kartoituksessa havaittiin, että tietoturva on pääosin hyvällä tasolla ja käytännön asiat on mietitty tarkoin. Koska kyseessä on suuri kansainvälinen yritys, kartoitusta ei pystytty toteuttamaan niin laajana kuin se pitäisi todellisuudessa toteuttaa. Tästä johtuen esimerkiksi fyysiseen tietoturvaan ei voida ottaa kantaa suuremmassa mittakaavassa.

Käytännön testausosuudessa tehtiin yrityksen sisäverkkoon ja työasemaan kohdistuvia testauksia. Testauksissa saatiin selville että tietoturva on näiltä osin mietitty todella pitkälle, mutta joitain heikkouksiakin löydettiin. Suurimmat tietoturvariskit nähtiin olevan se, että käytössä on vielä pian vanhentuvia palvelinkäyttöjärjestelmiä ja verkon kriittisimmille alueille ei ole pääsyrajoituksia. Tarkoituksena oli myös testata löydettyjen haavoittuvuuksien hyödyntämistä, mutta sen ei katsottu tässä olevan välttämätöntä koska yrityksen verkkoon tätä ei saatu tehdä ja hyökkäysohjelmistojen käyttö oli rajoitettua.

Yhteenvetona todetaan, että tehty työ vastasi hyvin tutkimuskysymyksin eli yrityksen tietoturvaa saatiin kartoitettua riittävän kattavasti. Työssä saatiin selville myös yrityksen tietoturvan puutteita, joihin pohdittiin parannusehdotuksia eli tavoitteet saatiin täytettyä.

Lähteet

1 Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WSOY.

2 Network Security Auditing. 2010. Verkkodokumentti. Cisco Press. <http://www.pdfiles.com/pdf/files/English/Security/Network_Security_Auditing.pdf>. Luettu 21.2.2015

3 Thomas, Tom. 2005. Verkkojen tietoturva. Helsinki: Edita.

4 McClure, S., Scambray, J. & Kurtz, G. 2009. Hacking Exposed. McGraw-Hill Osborne

5 P2P. 2015. Verkkodokumentti. Afterdawn. <http://fin.afterdawn.com/sanasto/selitys.cfm/p2p>. Luettu 8.3.2015.

6 Orebaugh, A. & Pinkard, B. 2008. Nmap in the Enterprise. Syngress Media

7 What's The Difference Between OSI Seven-Layer Network Model And TCP/IP? 2013. Verkkodokumentti. Electronic design. <http://electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip>. Luettu 14.3.2015.

8 DHCP. 2015. Verkkodokumentti. Linux.fi. <http://www.linux.fi/wiki/DHCP>. Luettu 14.3.2015.

9 Penetration Testing Execution Standard. 2014. Verkkodokumentti. PTES. <http://www.pentest-standard.org>. Luettu 21.2.2015.

10 Man In the Middle Attack. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Man-in-the-middle_attack>. Luettu 13.3.2015.

11 OSI-malli. 2015. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/OSI-malli>. Luettu 8.3.2015.

12 Kali Linux. 2015. Verkkodokumentti. Kali Linux. <https://www.kali.org>. Luettu 21.2.2015.

13 Crack and reset the system password locally using Kali Linux. 2014. Verkkodokumentti. Linux Digest. <https://sathisharthars.wordpress.com/2014/08/19/crack-and-reset-the-system-password-locally-using-kali-linux>. Luettu 7.4.2015.

14 Chntpw bug. 2012. Verkkodokumentti. Launchpad.net. <https://bugs.launchpad.net/ubuntu/+source/chntpw/+bug/1046622>. Luettu 9.4.2015.

15 Apache 2.0.44 haavoittuvuudet. 2014. Verkkodokumentti. CVE Details. <http://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-10691/Apache-Http-Server-2.0.44.html>. Luettu 9.4.2015.

16 Yritystapaaminen 26.3.2015 Vantaalla. Senior IT Manager & IT Manager